DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

11 FEB 2003

MEMORANDUM FOR SEE DISTRIBUTION

FROM: HQ AFMC/IT
4225 Logistics Avenue, Room N136
Wright-Patterson AFB OH 45433-5772

SUBJECT: AFMC Policy Regarding Use of the DoD Public Key Infrastructure (PKI)

1. AFMC is well on its way to implementing the DoD PKI. Personnel at AFMC locations exchange digitally signed and/or encrypted e-mail, authenticate to Public Key-enabled applications and websites, and logon to the network using their PKI certificates. By October 2003, the DoD will have issued new identification cards, Common Access Cards (CAC), to all eligible personnel. Loaded on the CAC are the person's DoD PKI certificates.

2. This memo provides instructions and guidelines on the use of DoD PKI certificates within AFMC (see attachment). Some directives regarding the use and protection of DoD PKI certificates also apply to the CAC itself because the certificates are stored on the CAC. The policies set in this memorandum are automatically superseded by published DoD or AF instructions and directives that address the same subject.

3. My point of contact is Mr. Dennis S. Hernit, HQ AFMC/ITXC, DSN 986-0650, commercial (937) 656-0650, e-mail: dennis.hernit@wpafb.af.mil.

Kenneth Percell

KENNETH I. PERCELL, SES
Director
Information Technology

Attachment:
AFMC Policy on use of the DoD Public Key Infrastructure

DISTRIBUTION:
(ALHQCTR)

(Field CCs)
AAC/CC
AEDC/CC
AFFTC/CC
AFRL/CC
AFSAC/CC
AMARC/CC
ASC/CC
ESC/CC
OC-ALC/CC
OO-ALC/CC
USAFM/DIR
WR-ALC/CC
311 HSW/CC
377 ABW/CC
88 ABW/CC

(Field SCs)
AEDC/SDC
AFFTC/IT
AFRL/IFOS
AMARC/XPI
SSG/SC
66 ABW/SC
72 CS/CC
75 CS/CC
78 CS/CC
88 CG/CC
96 CG/CC
311 CS/CC
377 CS/CC

OTHER:
JDMAG/MAA

AFMC Policy on Use of the DoD Public Key Infrastructure (PKI)

1. Any person, application, or system that requires support from a PKI must use the DoD PKI unless explicit approval is granted by the DoD PKI Program Management Office.

   a. This applies, but is not limited, to user, device, code-signing, and server certificates.

   b. This does not apply to the Defense Message System High Grade Service which uses its own PKI to generate FORTEZZA cards.

2. Persons to whom DoD PKI certificates are issued must protect those PKI certificates and their associated personal identification numbers (PIN) IAW the DoD PKI Certificate Policy and Air Force Systems Security Instruction 3034, *FORTEZZA User Requirements (FOUO).* Appropriate protection must also be afforded the token (e.g., the CAC or a floppy disk) on which the DoD PKI certificates are stored.

3. In accordance with the DoD Chief Information Officer (CIO) mandate, all AFMC organizations must perform the following as soon as possible but no later than October 2003:

   a. E-mail sent within the DoD must be digitally signed. This applies to all unclassified e-mail sent from one .mil e-mail address to another.

   b. All private DoD and DoD-interest webservers must enable client authentication.

   (1) Private webservers are those that contain information not releasable to the general public or is intended only for a subset of the entire DoD or AF. An example of the former would be a base's home page accessible by anyone in the .mil or .gov domain. An example of the latter is the web-enabled base phone directory available only to people on that base.

   (2) HQ AFMC/IT directed that web content must be migrated onto the Air Force Portal and that the physical webservers be shut down or re-utilized. Doing so will satisfy the DoD CIO mandate because the AF Portal will perform client authentication before access is granted.

   c. All unclassified networks must be enabled for hardware token, PKI certificate-based network logon. The hardware token in this case is the CAC.

4. USAF and USAF-contracted developers of applications and systems intended for the AF must consider use of PKI certificates if the application or system requires identification and authentication of its users. The DoD as a whole is moving away from the traditional user ID and password and towards two-factor authentication made possible by PKI certificates and PINs.

5. Organizations purchasing Public Key-enabled commercial off-the-shelf products must ensure that these products are compatible with the DoD PKI, the tokens on which the PKI certificates are stored (CAC, floppy disk, universal serial bus plugs, etc.), and the hardware/software used to access the PKI certificates.

6. The AFMC public key infrastructure, which uses a Microsoft certification authority, will issue only device certificates. No user certificates will be issued from the AFMC PKI. All user certificates will be issued from the DoD PKI.

7. While there is no mandate regarding its use, encryption of e-mail is highly encouraged especially when transmitting unclassified but sensitive information via the NIPRNET. Examples of this type of information include social security numbers, itineraries of high-ranking personnel, and recall rosters.